UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/081,500	02/22/2002	John Owlett	GB920010095US1	1505

46590 7590 09/19/2006

MYERS BIGEL SIBLEY SAJOVEC P.A.
PO BOX 37428
RALEIGH, NC 27627

EXAMINER	
LAFORGIA, CHRISTIAN A	
ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 09/19/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/081,500
Filing Date: February 22, 2002
Appellant(s): OWLETT, JOHN

Timothy Wall (Reg. No. 50,743)
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 14 June 2006 appealing from the Office action mailed 24 January 2006.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

2002/01034301	ANDERSSON	03-2002
2004/0202328	HARA	10-2004
6,072,875	TSUDIK	06-2000

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 1-5 and 11-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Application Publication No. 2002/0034301 to Andersson, hereinafter Andersson, in view of U.S. Application Publication No. 2004/0202328 to Hara, hereinafter Hara.

As per claims 1, 13, and 14, Andersson discloses a method for authentication of a user by an authenticating entity comprising the steps of:

the authenticating entity sending a challenge to the user (page 3, paragraph [0040], i.e. the authentication server issues a challenge to the user);

the user encrypting the challenge using a private key of an asymmetric key pair (page 3, paragraph [0040], i.e. the authentication token encrypts the challenge with the user's private key);

the user sending a response to the authenticating entity in the form of the encrypted challenge (page 3, paragraph [0040], i.e. the authentication token encrypts the challenge with the user's private key, and returns it to the authentication server).

Andersson does not disclose the user adding a spoiler to the challenge and encrypting the combined spoiler and challenge.

Hara discloses adding padding to data and encrypting the data and the padding information (Figures 7b, 7c, page 5, paragraphs [083], [0084]).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to add padding data to the password and encrypting the password with the padding data, since Hara discloses at page 5, paragraphs [083], [0084] that padding data makes it better suited for encryption, as it is known that padding data to a certain length makes the encryption stronger, which is desirable when trying to prevent transmitted password information from being intercepted.

Regarding claim 2, Andersson teaches wherein the method includes the authenticating entity decrypting the encrypted combined spoiler and challenge using the public key of the asymmetric key pair and determining if the user has been authenticated (page 3, paragraph [0040], i.e. the returned challenge is then decrypted by the authentication server with the user's public key).

Regarding claim 3, Hara teaches wherein the addition of spoiler to the challenge is carried out by applying spoiler function to the challenge (Figures 7b, 7c, page 5, paragraphs [083], [0084]).

With regards to claim 4, Hara teaches wherein the form the spoiler function is sent to the authenticating entity (Figures 7b, 7c, page 5, paragraphs [0084], i.e. knowing where the padding is located in order for it to be removed later).

Regarding claim 5, Hara discloses wherein the spoiler is added to the challenge as a prefix or a suffix and the authenticating entity extracts the challenge by counting the number of bytes from the beginning or end of the combined spoiler and challenge (page 5, paragraphs [0084]).

Regarding claim 11, Andersson teaches wherein the challenge is a bit sequence (page 1 paragraph [0007], i.e. Wireless Application Protocol transmits data in binary sequence).

Regarding claim 12, Hara discloses wherein the spoiler is an additional bit sequence (page 5, paragraphs [083], [0084]).

Claims 6-8 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Andersson in view of Hara as applied above, and further in view of U.S. Patent No. 6,072,875 to Tsudik, hereinafter Tsudik.

Regarding claim 6, Andersson and Hara do not wherein the method includes the user obtaining a digest of the combined spoiler and challenge before the step of encrypting.

Tsudik teaches wherein the method includes the user obtaining a digest of the challenge before the step of encrypting (column 3, line 59 to column 4, line 11).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to obtain a digest of the combined spoiler and challenge, since Tsudik states at column 4, lines 12-21 that such a modification would allow for mobile users while minimizing the traceability and possibility of identifying the mobile user.

With regards to claim 7, Tsudik discloses wherein the user obtains the digest by applying a hash function to the combined spoiler and challenge (column 3, line 59 to column 4, line 11).

With regards to claim 8, Tsudik teaches wherein the user sends details of the spoiler and the method of obtaining the digest to the authenticating entity (column 6, lines 42-63, i.e. home domain authority keeps track of user).

Regarding claim 9, Tsudik teaches wherein the user sends details of the algorithm used for encryption to the authenticating entity (column 5, lines 27-48).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to send details of the encryption to be used by mobile users, since Tsudik states at column 4, lines 12-21 that such a modification would allow for mobile users while minimizing the traceability and possibility of identifying the mobile user.

Concerning claim 10, Tsudik discloses wherein the authenticating entity obtains a digest of the combined spoiler and the original challenge that the authenticating entity sent to the user and compares the digest a digest obtained by decrypting the response from the user (column 3, line 59 to column 4, line 11).

(10) Response to Argument

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies, such as the security benefits of a spoiler, are not recited in the rejected claims. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies, such as a spoiler function, are not recited in the rejected claims. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

In response to applicant's argument that the spoiler adds a level of security, a recitation of the intended use of the claimed invention must result in a structural difference between the claimed invention and the prior art in order to patentably distinguish the claimed invention from the prior art. If the prior art structure is capable of performing the intended use, then it meets the claim.

In response to the Applicant's argument that the cited references do not teach adding a spoiler to the challenge, the Examiner disagrees. The Applicant defines a spoiler on page 8 of the specification as "be[ing data] added to the challenge as a prefix or a suffix and the authenticating entity extracts the challenge by counting the number of bytes from the beginning or end of the combined spoiler and challenge." *Hara* discloses adding padding to data and then encrypting the data along with the padding data, because the data is then better suited for encryption (see **Grounds of Rejection** and paragraphs 83 and 84).

In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d

1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, the references themselves provide a teaching of the benefits of adding padding data, or a spoiler, as cited in the Office Action of 24 January 2006 and again above. *Hara* suggests to one of ordinary skill in the art in paragraphs 83 and 84 that adding padding information, or a spoiler, to data makes it better suited for encryption, in particular triple-DES, one of the strongest known public key cryptosystems, and easier to implement for high-speed encryption on a hardware basis.

In response to applicant's argument that the examiner's conclusion of obviousness is based upon improper hindsight reasoning, it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971).

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Christian LaForgia
Patent Examiner
Art Unit 2131

Conferees:
Gilberto Barron
Supervisory Patent Examiner
Art Unit 2132

Benjamin Lanier
Patent Examiner
Art Unit 2132

Gilberto, B

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100